Today's Presentation:

Creating a "hands-on" Security Compliance course

PCCCyber

Speaker Bio

- Born in Louisiana
- Relocated in 1994 to North Carolina
- Attended East Carolina University
- Employed as Systems Administrator (~10 years)
- Currently teaching at Pitt Community College (14 years)
- Moved into Cyber Realm in 2016
- Certs include: CEH, CCNA CyberOps, SSCP, PCNSA

College Bio

- Pitt Community College
- Winterville, NC
- Chartered by the State Board of Education in March 1961
- Offer diplomas and certificates for more than 60 programs
- Serve more than 23,000 credit and non-credit students annually
- 6th largest in N.C. Community College System in terms of student credit hours
- Quality Matters member since 2016
- National Center of Academic Excellence in Cybersecurity since 2020

Agenda

- Project Background
  - Quality Matters
  - North Carolina Partnership for Cybersecurity Excellence (**NC-PaCE**)
  - Knowledge Gap
- Cyber Security Program
- Course Syllabus
- Course Content
- Course Labs
- Sponsored Internships

Project Background

Quality Matters

Quality Matters Rubric

QUALITY MATTERS

QM

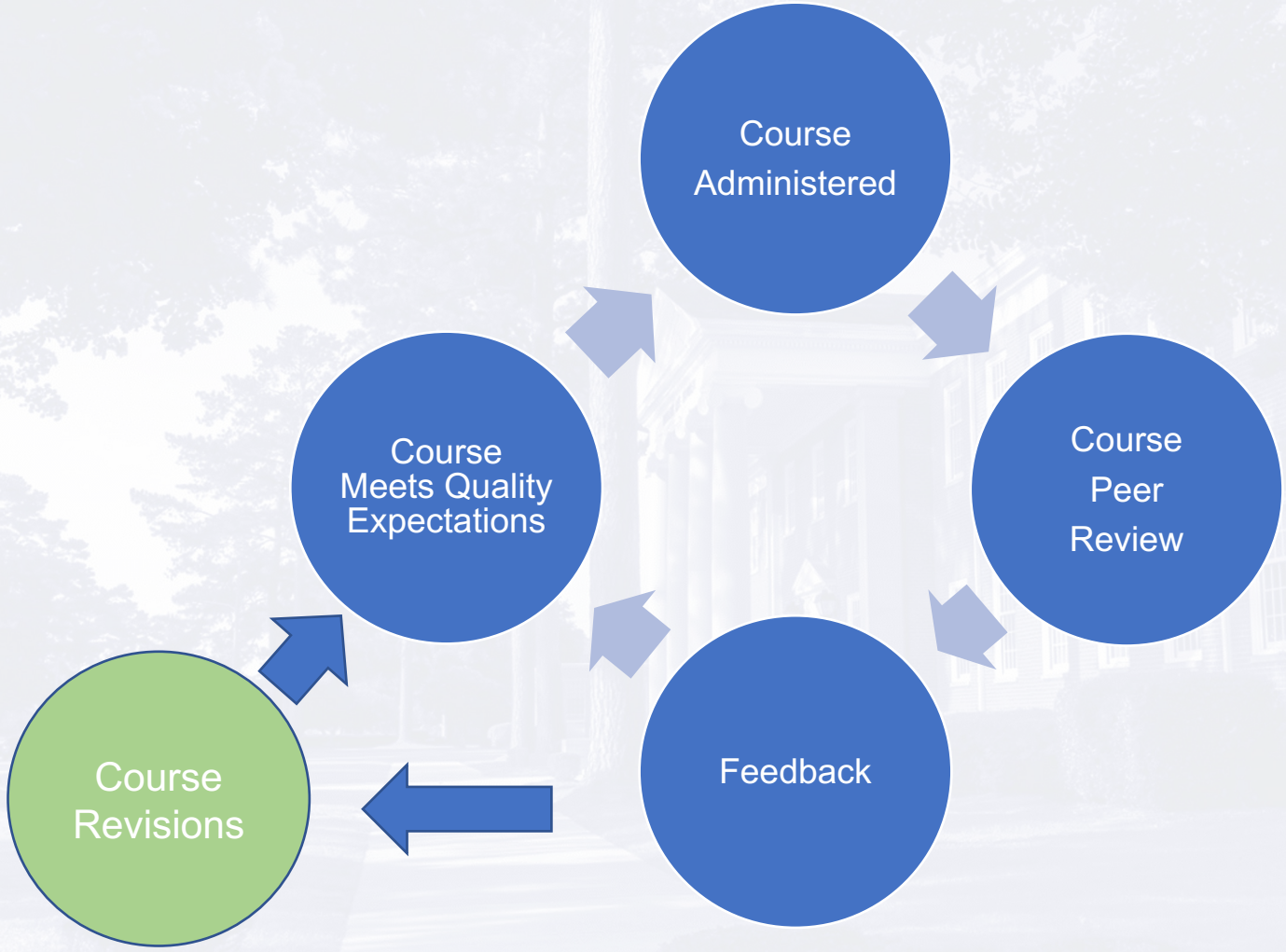
Standards from the QM Higher Education Rubric, Fifth Edition

For more information visit www.qualitymatters.org or email info@qualitymatters.org

Standards		Points
Course Overview Introduction	1.1 Instructions make clear how to get started and where to find various course components.	3
	1.2 Learners are introduced to the purpose and structure of the course.	3
	1.3 Etiquette expectations (sometimes called "netiquette") for online discussions, email, and other forms of communication are clearly stated.	2
	1.4 Course and/or institutional policies with which the learner is expected to comply are clearly stated, or a link to current policies is provided.	2
	1.5 Minimum technology requirements are clearly stated and instructions for use provided.	2
	1.6 Prerequisite knowledge in the discipline and/or any required competencies are clearly stated.	1
	1.7 Minimum technical skills expected of the learner are clearly stated.	1
	1.8 The self-introduction by the instructor is appropriate and is available online.	1
	1.9 Learners are asked to introduce themselves to the class.	1
Learning	2.1 The course learning objectives, or course/program competencies, describe outcomes that are measurable.	3

http://go.joeteach.us/3blwTxa

QM Course Review Process



Knowledge Gaps

- Advisory Board identified compliance as a critical “knowledge gap” in the current workforce as well as with students graduating
- NC-PaCE members identified compliance as a critical “knowledge gap”
- Collaboration with Richmond Community College also identified Information Security compliance as a knowledge gap.

NC-PaCE

Public and Private Working Together

- $2 million grant from the NCAE in Cybersecurity located within the National Security Agency
- Brought eight of North Carolina's universities and community colleges together
- Address a growing workforce gap / establish cybersecurity as an economic development tool for the state through education, research, services and outreach
- Giving North Carolina businesses the skilled workers, knowledge and support that they need to grow
- NC PaCE will be headquartered in NC State's Secure Computing Institute (SCI)
- Partners Include East Carolina University, North Carolina A&T State University, UNC Charlotte, UNC Wilmington and Forsyth, Wake and Pitt community colleges
- Pitt Community College will participate in sponsored internships
- Funding for Certification Exam Attempts by our Cybersecurity Students

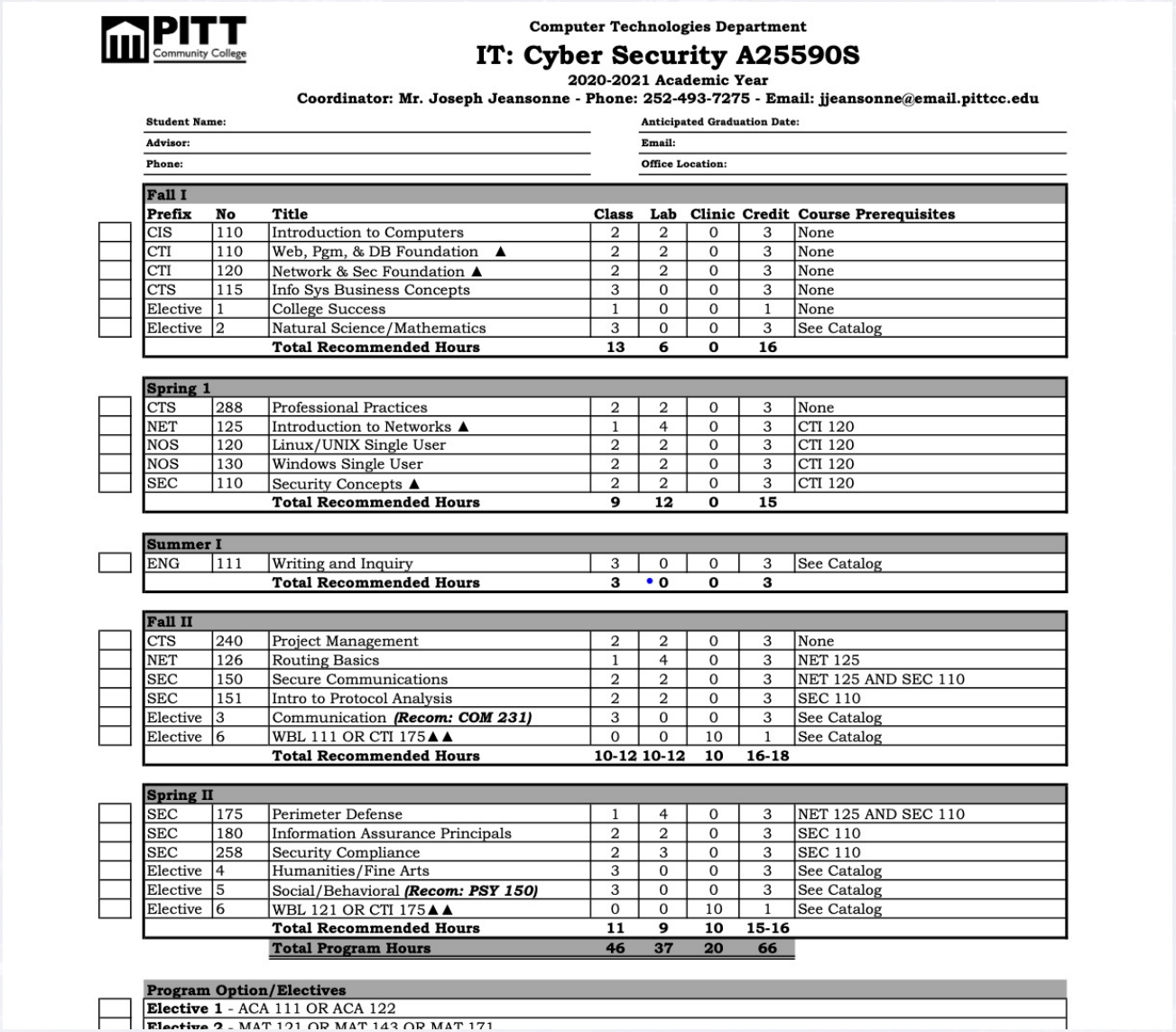
*https://www.engr.ncsu.edu/news/2021/10/01/statewide-cybersecurity-coalition-receives-2-million-nsa-grant/

Cyber Security Program

at Pitt Community College

Cyber Security Course Offerings

- Courses are offered TR, IN, HY
- Courses are typically offered once per year
- Program is 66 credit hours
- Courses are offered during the day and at night
- Students can choose between co-op and CWNP course
- 87 students currently enrolled
- 5 set to graduate this semester
- Networking Heavy



PITT Community College

Computer Technologies Department

IT: Cyber Security A25590S

2020-2021 Academic Year

Coordinator: Mr. Joseph Jeansonne - Phone: 252-493-7275 - Email: jjeansonne@email.pittcc.edu

Student Name: **Anticipated Graduation Date:**

Advisor: **Email:**

Phone: **Office Location:**

	Prefix	No	Title	Class	Lab	Clinic	Credit	Course Prerequisites
Fall I								
	CIS	110	Introduction to Computers	2	2	0	3	None
	CTI	110	Web, Pgm, & DB Foundation ▲	2	2	0	3	None
	CTI	120	Network & Sec Foundation ▲	2	2	0	3	None
	CTS	115	Info Sys Business Concepts	3	0	0	3	None
	Elective	1	College Success	1	0	0	1	None
	Elective	2	Natural Science/Mathematics	3	0	0	3	See Catalog
			Total Recommended Hours	**13**	**6**	**0**	**16**	
Spring 1								
	CTS	288	Professional Practices	2	2	0	3	None
	NET	125	Introduction to Networks ▲	1	4	0	3	CTI 120
	NOS	120	Linux/UNIX Single User	2	2	0	3	CTI 120
	NOS	130	Windows Single User	2	2	0	3	CTI 120
	SEC	110	Security Concepts ▲	2	2	0	3	CTI 120
			Total Recommended Hours	**9**	**12**	**0**	**15**	
Summer I								
	ENG	111	Writing and Inquiry	3	0	0	3	See Catalog
			Total Recommended Hours	**3**	**0**	**0**	**3**	
Fall II								
	CTS	240	Project Management	2	2	0	3	None
	NET	126	Routing Basics	1	4	0	3	NET 125
	SEC	150	Secure Communications	2	2	0	3	NET 125 AND SEC 110
	SEC	151	Intro to Protocol Analysis	2	2	0	3	SEC 110
	Elective	3	Communication ***(Recom: COM 231)***	3	0	0	3	See Catalog
	Elective	6	WBL 111 OR CTI 175▲▲	0	0	10	1	See Catalog
			Total Recommended Hours	**10-12**	**10-12**	**10**	**16-18**	
Spring II								
	SEC	175	Perimeter Defense	1	4	0	3	NET 125 AND SEC 110
	SEC	180	Information Assurance Principals	2	2	0	3	SEC 110
	SEC	258	Security Compliance	2	3	0	3	SEC 110
	Elective	4	Humanities/Fine Arts	3	0	0	3	See Catalog
	Elective	5	Social/Behavioral ***(Recom: PSY 150)***	3	0	0	3	See Catalog
	Elective	6	WBL 121 OR CTI 175▲▲	0	0	10	1	See Catalog
			Total Recommended Hours	**11**	**9**	**10**	**15-16**	
			Total Program Hours	**46**	**37**	**20**	**66**	

Program Option/Electives
Elective 1 - ACA 111 OR ACA 122
Elective 2 - MAT 121 OR MAT 143 OR MAT 171

Professional Cert Mappings

Preparing Global Workforce

CTI 120 Network & Sec Foundation
MTA Exam 98-366 Networking Fundamentals

CTI 175 Intro to Wireless Technology
CWNP Certified Wireless Technician

NET 125 Introduction to Networks
Cisco Certified Network Associate (200-301 CCNA)

NET 126 Switching, Routing, and Wireless Essentials
Cisco Certified Network Associate (200-301 CCNA)

NOS 120 Linux/UNIX Single User
Red Hat® Certified System Administrator (RHCSA)

NOS 130 Windows Single User
Microsoft Exam MD-100: Windows 10

SEC 110 Security Concepts
Comptia Security +

SEC 150 Secure Communications
CCNA Security

SEC 151 Intro to Protocol Analysis
Wireshark Certified Network Analyst Exam

SEC 175 Perimeter Defense
Palo Alto Certified Network Security Administrator (PCNSA)

SEC 180 Information Assurance Prin
Cisco Certified CyberOps Associate

Course Syllabus

NCCCS Course Description

SEC 258: Security Compliance

CIS Course ID		S24509	
Effective Term		Spring 2016	
Class	2	Lab	3
Clinical	0	Work	0
Credit	3		

This course introduces information security compliance and standards along with how they apply to corporate IT environments.

Topics include **ISO standards**, government **NIST frameworks**, federal and state compliance requirements, **security policies**, **incident response** and business **continuity planning**.

Upon completion, students should be able to apply compliance and availability requirements to corporate data enterprise scenarios.

https://www.pcmag.com/news/how-businesses-can-stay-on-top-of-changing-compliance-regulations

Required Text

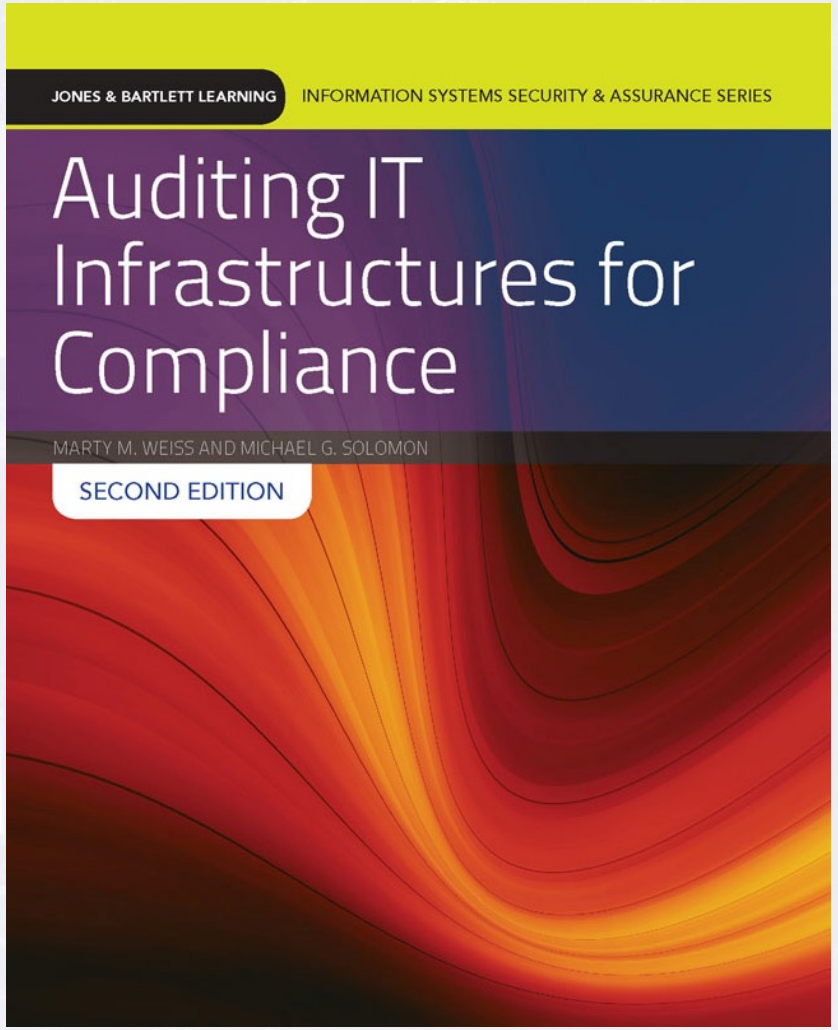
Auditing IT Infrastructures for Compliance

2016 - Second Edition

Martin Weiss / Michael Soloman

ISBN 978-1-284-09070-3 (pbk.)

$30

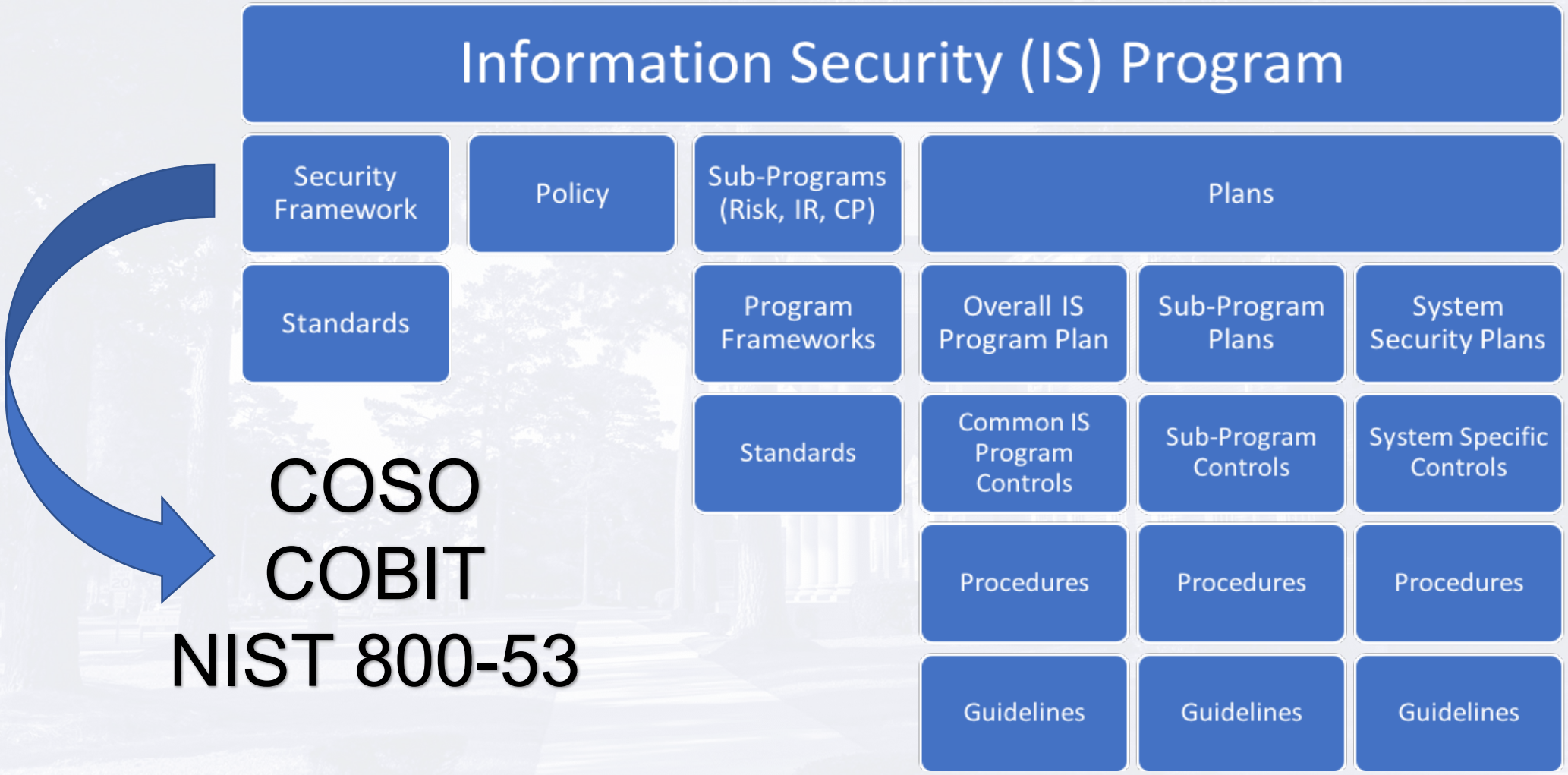


Course Outline

- The Need for Information Systems Security Compliance
- Overview of U.S. Compliancy Laws
- What Is the Scope of an IT Compliance Audit?
- Auditing Standards and Frameworks
- Planning an IT Infrastructure Audit for Compliance
- Conducting an IT Infrastructure Audit for Compliance
- Writing the IT Infrastructure Audit Report
- Compliance Within the User Domain
- Compliance Within the Workstation Domain
- Compliance Within the LAN Domain
- Compliance Within the LAN-to-WAN Domain
- Compliance Within the WAN Domain
- Compliance Within the Remote Access Domain
- Compliance Within the System/Application Domain
- Ethics, Education, and Certification for IT Auditors

SEC 258 – Sample Regulations Covered

SEC 258 – Compliance Frameworks



https://www.impactmakers.com/blog/infosec-taxonomy/

SEC 258 – Corporate Governance

https://stock.adobe.com/search?k=governance&asset_id=99367881

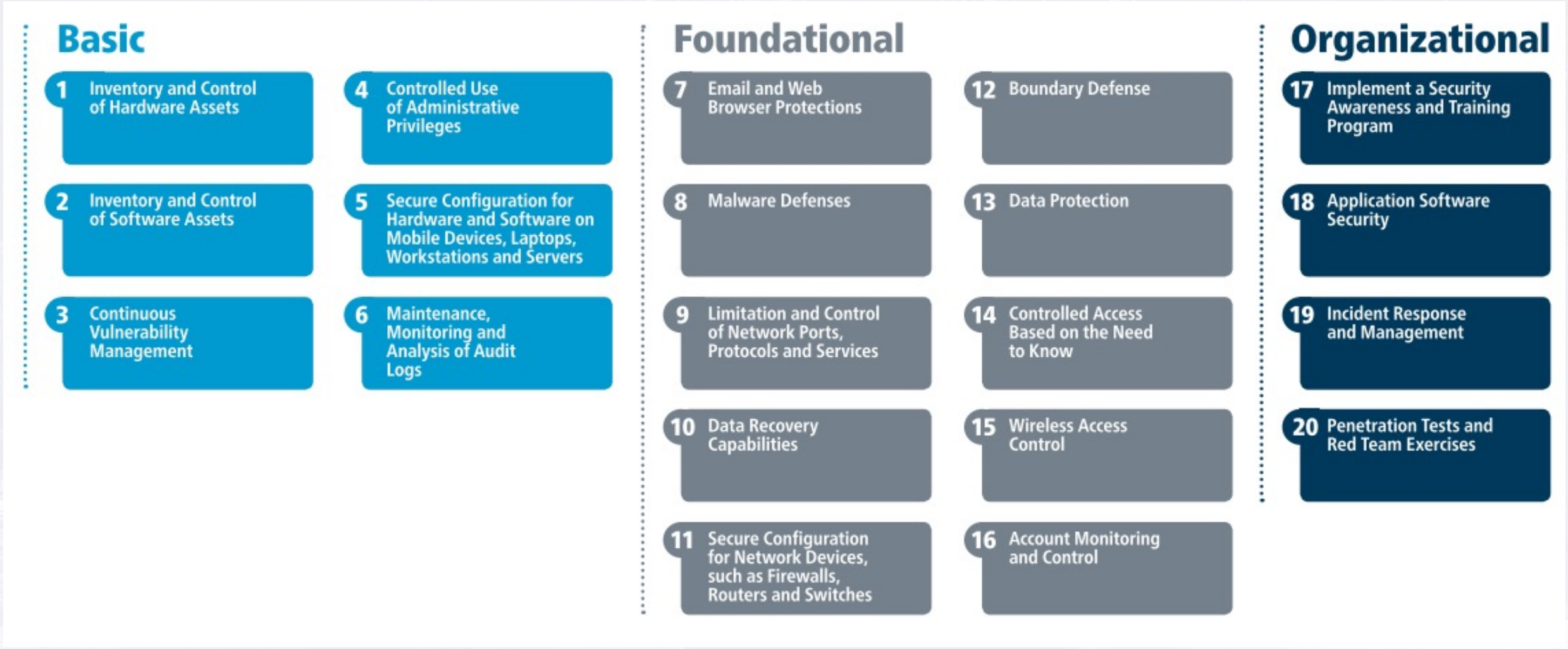
SEC 258 – Reducing Liability

https://go.joeteach.us/3bTyNLr

SEC 258 – Administrative Controls

https://www.forbes.com/sites/edwardsegal/2021/06/11/labor-departments-new-regulatory-agenda-what-it-means-for-businesses/?sh=75beab512f43

SEC 258 – Critical Controls / Maturity Levels



SEC 258 - Sample Project

Project Scenario

ACME Healthcare is a healthcare company that runs over 25 medical facilities including patient care, diagnostics, outpatient care and emergency care. The organization has experienced several data breaches over the last five years. These data breaches have cost the organization financially and damaged its reputation.

The executive leadership team recently hired a new Chief Information Security Officer (CISO). The new CISO has brought in one of the top cybersecurity penetration teams to perform a full security audit on the entire organization. This independent contractor conducted the audit, and found the following vulnerabilities:

1. Several accounts were identified for employees that are no longer employed by ACME.
2. Several user accounts allowed unauthorized and escalated privileges and accessed systems and information without formal authorization.
3. Several devices and systems allowed unsecure remote access.
4. Forty percent of all organization passwords audited were cracked within 6 hours.
5. Password expiration was not standardized.
6. Sensitive files were found unencrypted on user systems and laptops.
7. Several wireless hotspots used WEP for encryption and authentication.
8. Evidence indicates that sensitive e-mail was sent unencrypted to and from employee homes and mobile devices.

SEC 258 - Sample Project

Project Overview

This project includes the following tasks:

1. Review and prioritize scenario audit observations
2. Develop an information security policy and related procedure
3. Develop an implementation and dissemination plan

Objective: Developing Information Security Policies

A security policy is the document developed by an organization that formally states how it plans to protect its information and information systems. Organizations should treat a security policy as a "living document." This means that the organization continuously reviews and updates the document as technology and employee requirements change.

Organizations use several documents to support its policy infrastructure. In this project, you will be developing the following documents:

- An Information Security Policy
- A procedure to support the policy

An effective security policy references the standards and guidelines that exist within an organization. An information security policy contains high-level statements with the intent of protecting information and assets. It is the responsibility of senior management to develop security policies.

SEC 258 - Sample Project

ASSIGNMENT

CWUD: Awareness Poster

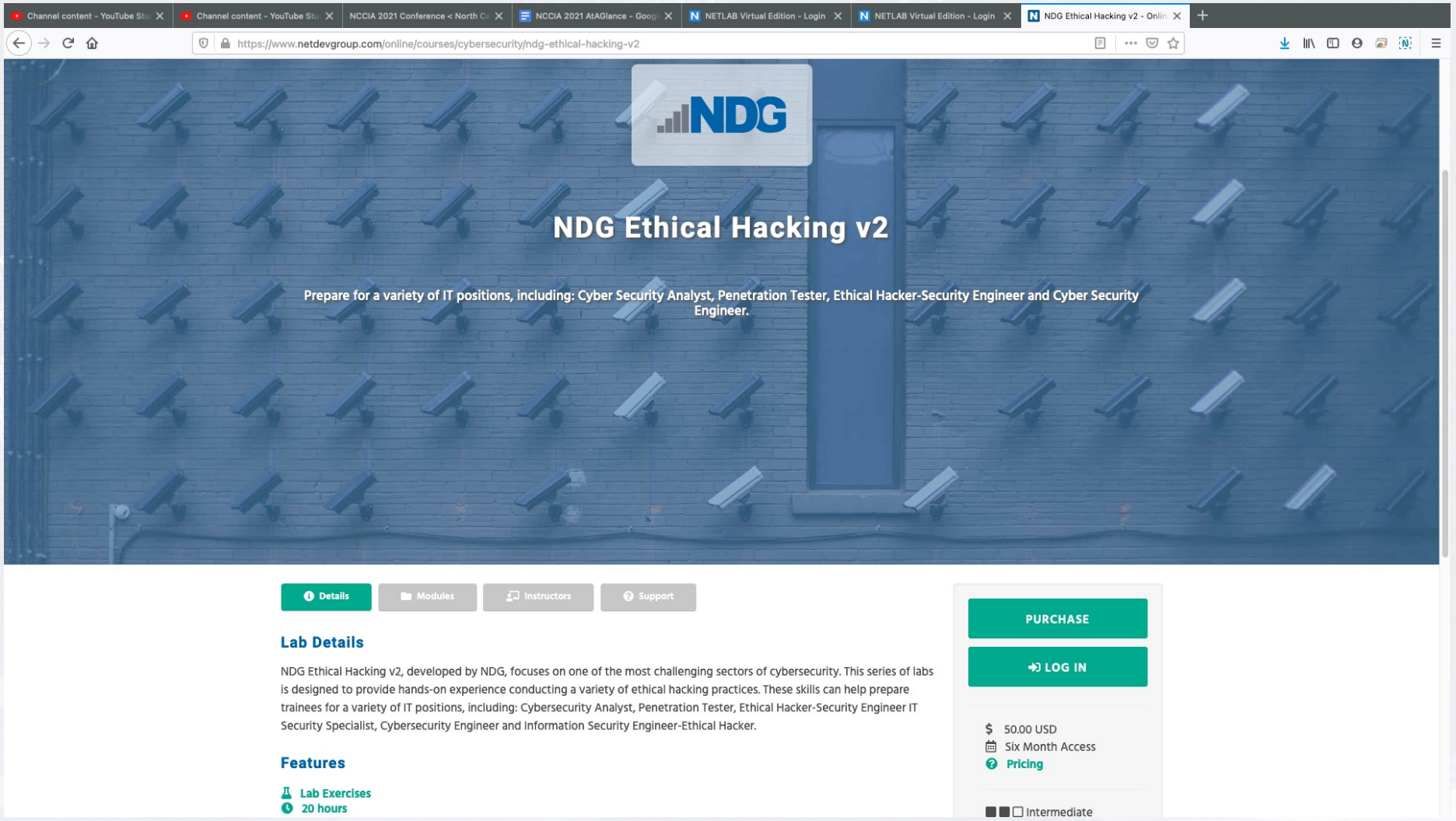
National Cyber Security Awareness Month (NCSAM) is observed in October in the United States of America. Started by the National Cyber Security Division within the Department of Homeland Security and the nonprofit National Cyber Security Alliance, the month raises awareness about the importance of cybersecurity. ACME Corp is sponsoring a Cyber Security Awareness Month Program this October and they would like for you to create an awareness poster to be displayed throughout the company.

Sample Submission:

SEC 258 - Course Labs

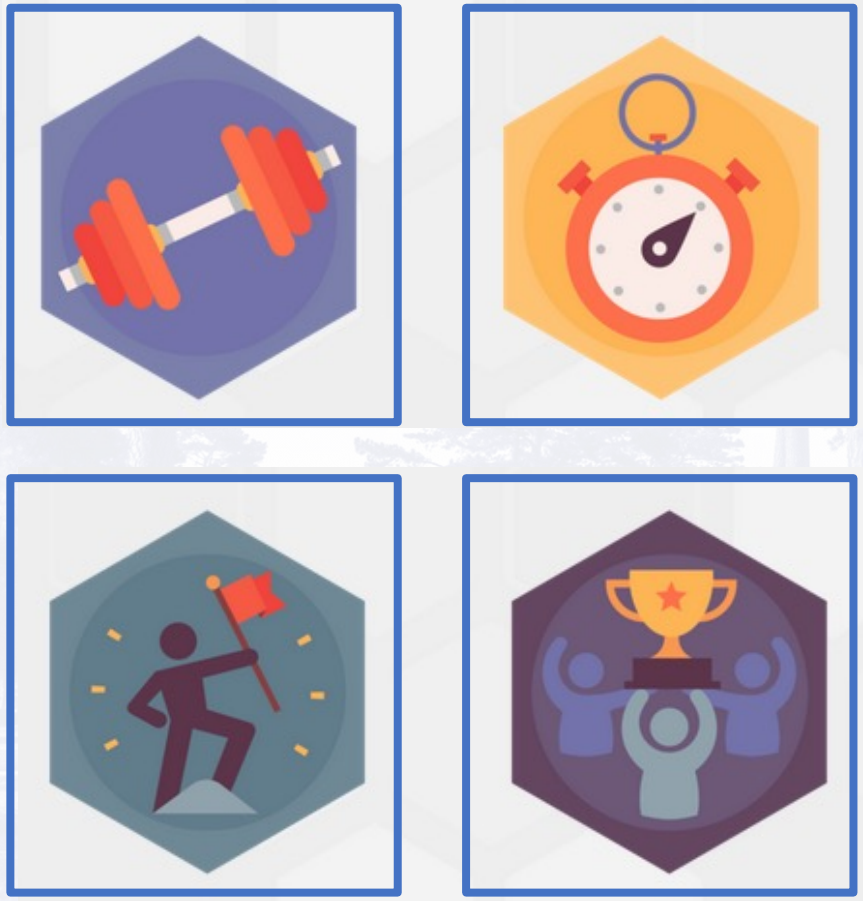
Chapter 4: Auditing Standards and Frameworks	Host Hardening
Chapter 5: Planning an IT Infrastructure Audit for Compliance	Digital Forensic Analysis
Chapter 6: Conducting an IT Infrastructure Audit for Compliance	Analyzing Network Packets
Chapter 7: Writing the IT Infrastructure Audit Report	Understanding SQL Commands and Injections
Chapter 8: Compliance Within the User Domain	Social Engineering Attacks with SET
Chapter 9: Compliance Within the Workstation Domain	Password Cracking with JTR and Hashcat
Chapter 10: Compliance Within the LAN Domain	Vulnerability Scanning with OpenVAS
Chapter 11: Compliance Within the LAN-to-WAN Domain	Evading IDS
Chapter 12: Compliance Within the WAN Domain	Reconnaissance with Nmap, Zenmap, and Masscan
Chapter 13: Compliance Within the Remote Access Domain	Extracting Data from a Compromised Machine
Chapter 14: Compliance Within the System/Application Domain	Client-Side Exploitations

NDG Hosted Option



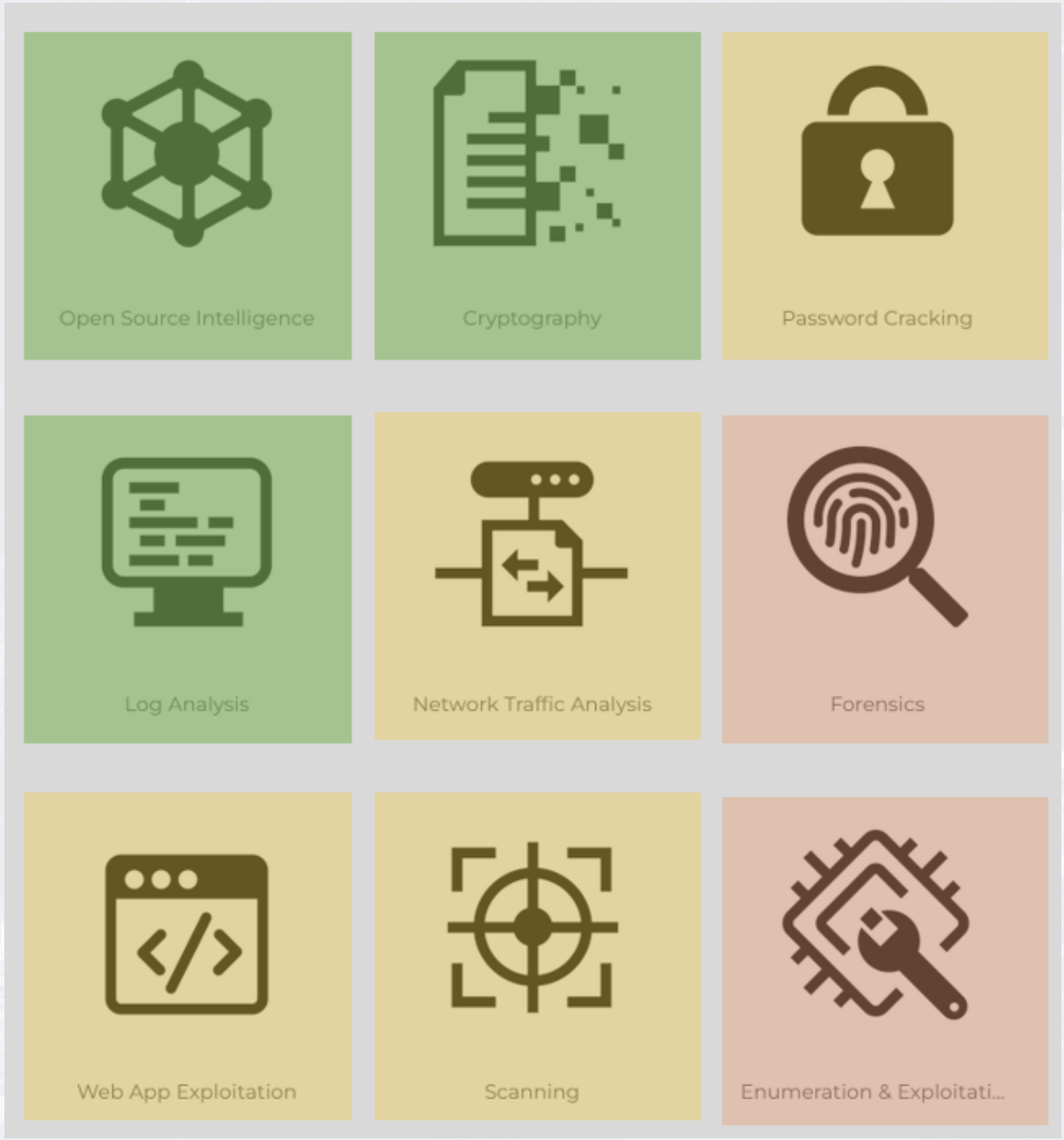

NCL
POWERED BY
CYBER SKYLINE

Areas of participation



National Cyber League Areas

- Gymnasium (Jan. 31 - May. 27)
- Practice Game (Mar. 28 - Apr. 4)
- Individual Game (Apr. 8 - Apr. 10)
- Team Game (Apr. 22 - Apr. 24)

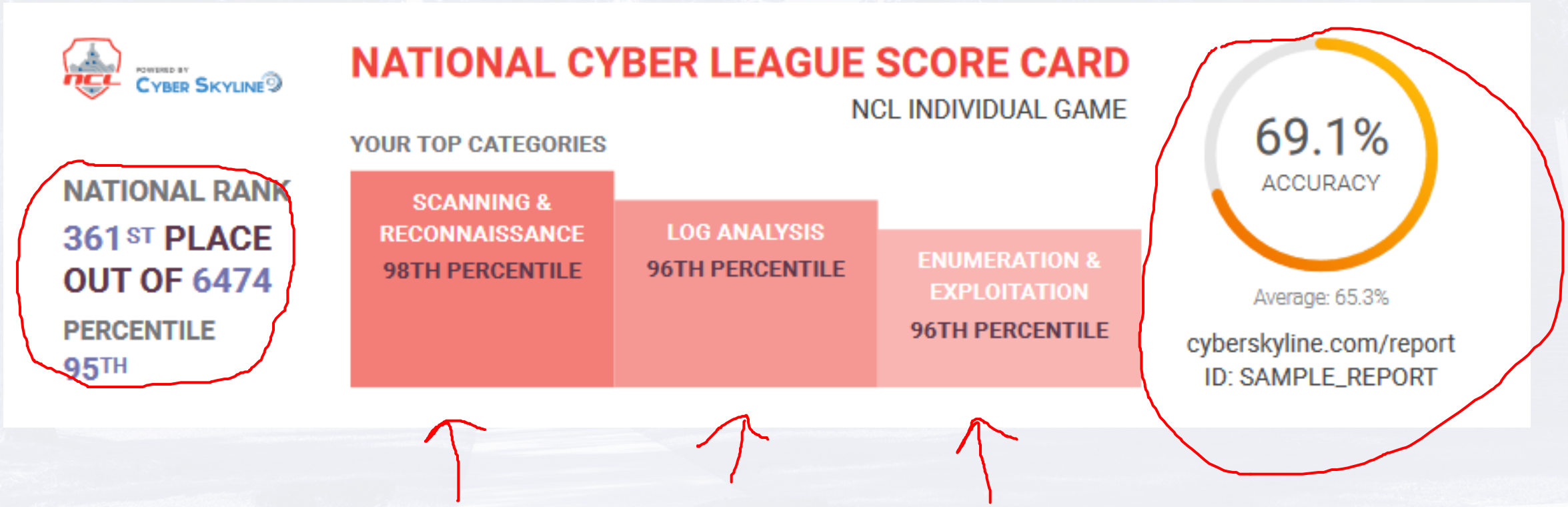


9 NCL Domains

- **Open Source Intelligence:** Utilize public information to gain knowledge on a target.
- **Cryptography:** Identify techniques used to encrypt messages, and extract the plain text.
- **Password Cracking:** Identify types of password hashes and determine plain text passwords.
- **Log Analysis:** Utilize tools and techniques to identify malicious activities using log files.
- **Network Traffic Analysis:** Examine malicious and benign network traffic to find security breaches.
- **Forensics:** Analyze, process, recover, and investigate digital evidence in a computer-related incident.
- **Scanning:** Gain intelligence about a target's potential vulnerabilities by scanning.
- **Web Application Exploitation:** Use exploits to bypass the security in online services.
- **Enumeration and Exploitation:** Use exploits to bypass the security measures in compiled binaries.

Scouting Report

85% Average



Work Based Learning

“Sponsored Internships”

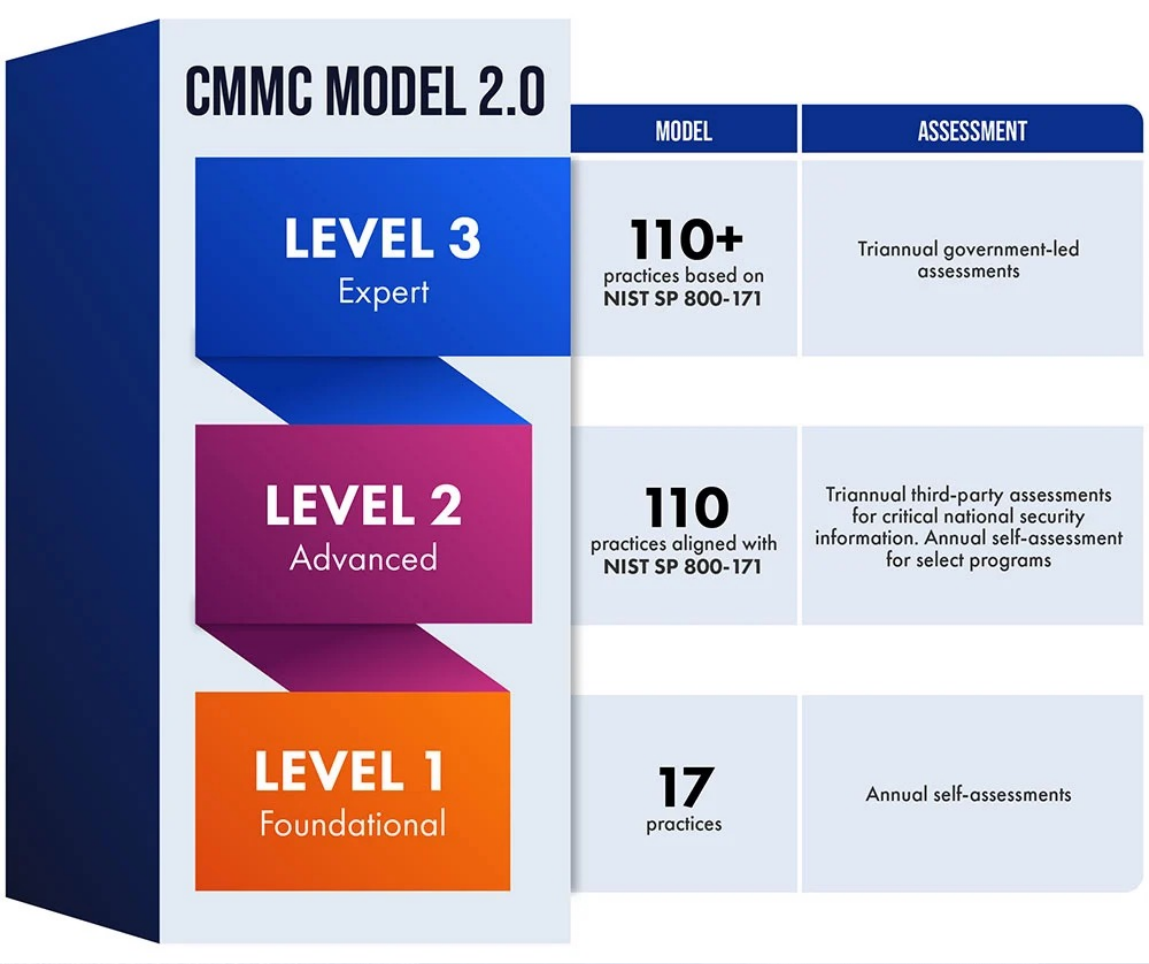
- Sponsored because they are students are being funded by the college via a grant (Student Win)
- No Cost to business except internship supervision
- Build out Cybersecurity capability were there is none
- “Drop In” Internship Projects
- Create a “fertile ground” so that Eastern North Carolina businesses can participate in Federal Government DoD projects (Industry Win)
- Develop new internship sites (Program Win)

Work Based Learning Project

CMMC Level 1 Assessment

PCCCyber

Cybersecurity Maturity Model Certification



- Level 1 (Foundational) allows organizations to demonstrate compliance through self-assessments
- Level 2 (Advanced) has bifurcated compliance expectations of both self assessment and independent auditing
- Level 3 (Expert) has government assessments every three years

https://www.celerium.com/cmmc-academy-for-defense-suppliers

WBL Project Model Example #1

- Submit a completed initial Cybersecurity Maturity Model Certification Level 1 assessment to my WBL Supervisor and my WBL faculty coordinator.
- Create a plan to resolve at least three security gaps identified by the initial Cybersecurity Maturity Model Certification Level 1 assessment.
- Submit a completed final Cybersecurity Maturity Model Certification Level 1 assessment to my WBL Supervisor and my WBL faculty coordinator.

WBL Project Model Example #2

- Research security awareness programs (SANS, etc.)
- Develop an employee survey on awareness (Assess Posture)
- Plan a security awareness campaign (Remediate)
- Evaluate group members (Assess Outcome)

Contact Info

Joseph Jeansonne

Pitt Community College

Winterville, NC

Dr. Greg Robison

Pitt Community College

Winterville, NC

- grobison@email.pittcc.edu
- www.pittcyber.org